DETAILED ACTION

This Examiner's Amendment and Examiner's Reasons for Allowance action is in response to the filing of 08/20/2010.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with David Millers on 11/05/2010.

- **The application's claims have been amended as follows:**

1. (Currently Amended) A data handling apparatus for a computer platform using an operating system executing a process, the apparatus comprising

a data management unit arranged to associate data management information with data input to the process and to regulate operating system operations involving the data according to the data management information;

a system call monitor implemented in the computer platform and operating to detect predetermined system calls and data manipulation by the process so as to modify identifiable characteristics of the data, wherein the system call monitor includes supervisor code that is executed within a program flow of the process, and

means for applying a data handling policy upon detecting:

(1) a predetermined data type based on a tag or label associated with the data manipulated by the process or based on [[the]] a format of the data manipulated by the process; and

(2) one of the predetermined system calls being detected, whereby the data handling policy is applied for all system calls involving the writing of data outside the process, wherein

the supervisor code controls the process at run time to administer the operating system data management unit.

2. (Canceled)

3. (Currently Amended) [[A]] The data handling apparatus according to claim 6, in which [[a]] the policy interpreter in its application of the policy automatically encrypts [[the]] at least [[some]] a portion of the data.

4. (Currently Amended) [[A]] The data handling apparatus according to claim 1, in which predetermined system calls are those involving the transmission of data externally of the computing platform.

5. (Currently Amended) [[A]] The data handling apparatus according to claim 1, in which the means for applying a data handling policy comprises a tag determiner for determining any security tags associated with data manipulated by the process or based on the format of the data manipulated by the process handled by the system call, and a policy interpreter for determining a policy according to any such security tags and for applying the policy.

6. (Currently Amended) [[A]] The data handling apparatus according to claim 5, in which the policy interpreter is configured to use the intended destination of the data as a factor in determining the policy for the data.

7. (Currently Amended) [[A]] The data handling apparatus according to claim 5, in which the policy interpreter comprises a policy database including tag policies and a policy reconciler for generating a composite policy from the tag policies relevant to the data.

8. (Canceled)

9. (Currently Amended) [[A]] The data handling apparatus according to ~~claim 8~~ claim 1, in which the computing platform further comprises a memory space, and is arranged to load the process into the memory space and run the process under the control of the data management unit.

10. (Currently Amended) [[A]] The data handling apparatus according to ~~claim 8~~ claim 1, in which the data management information is associated with at least one data sub-unit as data is input to a process from a data unit comprising a plurality of sub-units.

11. (Currently Amended) [[A]] The data handling apparatus according to ~~claim 8~~ claim 1, in which data management information is associated with each independently addressable data unit.

12. (Currently Amended) [[A]] The data handling apparatus according to ~~claim 8~~ claim 1, in which the data management unit comprises part of an operating system kernel space.

13. (Currently Amended) [[A]] The data handling apparatus according to claim 12, in which the operating system kernel space comprises a tagging driver arranged to control loading of the supervisor code into the memory space with the process.

14. (Canceled).

15. (Currently Amended) [[A]] The data handling apparatus according to ~~claim 14~~ claim 1, in which the supervisor code is arranged to analyze instructions of the process to identify operations involving the data, and, provide instructions relating to the data management information with the operations involving the data.

16. (Currently Amended) [[A]] The data handling apparatus according to claim 13, in which the memory space further comprises a data management information area under control of the supervisor code arranged to store the data management information.

17. (Currently Amended) [[A]] The data handling apparatus according to ~~claim 8~~ claim 1, in which the data management unit comprises a data filter to identify data management information associated with data that is to be read into the memory space.

18. (Currently Amended) [[A]] The data handling apparatus according to ~~claim 8~~ claim 1, in which the data management unit further comprises a tag management module arranged to allow a user to specify data management information to be associated with data.

19. (Currently Amended) [[A]] The data handling apparatus according to ~~claim 8~~ claim 1, in which the data management unit comprises a tag propagation module arranged to maintain an association with the data that has been read into the process and the data management information associated therewith.

20. (Currently Amended) [[A]] The data handling apparatus according to claim 19, in which the tag propagation module is arranged to maintain an association between an output of operations carried out within the process and the data management information associated with the data involved in the operations.

21. (Currently Amended) [[A]] The data handling apparatus according to claim 19, in which the tag propagation module comprises state machine automatons arranged to maintain an association between an output of operations carried out within the process and the data management information associated with the data involved in the operations.

22. (Currently Amended) A data handling method for a computer platform using an operating system executing a process, the method comprising the steps of:

associating data management information with data input to the process;

detecting in the computer platform both (i) a predetermined data type based on a tag or label associated with the data or based on [[the]] a format of the data and (ii) predetermined system calls involving the writing of data outside the process, and

applying a data handling policy to a system call upon both said predetermined data type and said a predetermined system call being detected, the data handling policy being applied for all system calls involving the writing of data outside the process; and

regulating operating system operations involving the data according to the data management information, wherein

supervisor code administers the method by controlling the process at run time.

23. (Currently Amended) [[A]] The data handling method according to claim 22, in which the policy is to require the encryption of at least [[some]] a portion of the data.

24. (Currently Amended) [[A]] The data handling method according to claim 23, in which in its application of the policy at least [[some]] a portion of the data is automatically encrypted.

25. (Currently Amended) [[A]] The data handling method according to claim 22, in which predetermined system calls are those involving the transmission of data externally of the computing platform.

26. (Currently Amended) [[A]] The data handling method according to claim 22, in which the method includes the steps of: determining any security tags associated with data handled by the system call, determining a policy according to any such tags and applying the policy.

27. (Currently Amended) [[A]] The data handling method according to claim 26, in which a composite policy is generated from the tag policies relevant to the data.

28. (Currently Amended) [[A]] The data handling method according to claim 26, in which the intended destination of the data is used as a factor in determining the policy for the data.

29. (Canceled)

30. (Canceled)

31. (Currently Amended) [[A]] The data handling method according to ~~claim 29~~ claim 22, in which the step (a) comprises associating data management information with data as the data is read into a memory space.

32. (Currently Amended) [[A]] The data handling method according to ~~claim 29~~ claim 22, in which the step (a) comprises associating data management information with at least one data sub-unit as data is read into a memory space from a data unit comprising a plurality of data sub-units.

33. (Currently Amended) [[A]] The data handling method according to ~~claim 29~~ claim 22, in which the step (a) comprises associating data management information with each independently addressable data unit that is read into the memory space.

34. (Currently Amended) [[A]] The data handling method according to ~~claim 29~~ claim 22, in which the data management information is written to a data management memory space under control of the supervisor code.

35. (Currently Amended) [[A]] The data handling method according to claim 34, in which the supervisor code comprises state machine automatons arranged to control the writing of data management information to the data management memory space.

36. (Currently Amended) [[A]] The data handling method according to ~~claim 29~~ claim 22, in which the step (b) comprises sub-steps

(b1) identifying an operation involving the data;

(b2) if the operation involves the data and is carried out within the process, maintaining an association between an output of the operation and the data management information; and

(b3) if the operation involving the data includes a write operation to a location external to the process, selectively performing the operation dependent on the data management information.

37. (Currently Amended) [[A]] The data handling method according to claim 36, in which, the step (b1) comprises: analyzing process instructions to identify operations involving the data; and, providing instructions relating to the data management information with the operations involving the data.

38. (Currently Amended) [[A]] The data handling method according to ~~claim 29~~ claim 22, in which the process instructions are analyzed as blocks, each block defined by operations up to a terminating condition.

39. (Currently Amended) [[A]] The data handling method according to claim 22, performed by the computer platform executing a computer program stored in computer readable media ~~for controlling a computing platform to operate in accordance with claim 22~~.

40. (Currently Amended) [[A]] The data handling method according to claim 22, performed by the computer platform ~~configured to operate according to claim 22~~.

41. (Currently Amended) A data handling apparatus for a computer platform using an operating system executing a process, the apparatus comprising:

a data management unit arranged to associate data management information with data input to the process and to regulate operating system operations involving the data according to the data management information;

a system call monitor implemented in the computer platform and operating to detect predetermined system calls and data handled by the process, wherein the system call monitor includes supervisor code that is executed within a program flow of the process and wherein the supervisor code controls the process at run time to administer the operating system data management unit, and

a policy ~~applicator~~ interpreter for applying a data handling policy to the system call upon both (i) a predetermined data type based on a tag or label associated with the data handled by the process or based on [[the]] a format of the data handled by the process and (ii) a predetermined system call which involves the writing of data outside the process.

Allowance

2. Claims 2, 8, 14, 29, & 30 have been cancelled.

3. Claims 1, 3-7, 9-13, 15-28, & 31-41 have been amended with written arguments which overcome the examiner's prior rejections and objections, see papers of 01/29/2010 & 07/22/2010. Examiner withdraws all outstanding rejections and objections to Claims 1, 3-7, 9-13, 15-28, & 31-41.

4. Claims 1, 3-7, 9-13, 15-28, & 31-41 are allowed.

Examiner's Statement of Reasons for Allowance

5. Prior art was found which disclosed robust encryption and decryption of packetized data transferred across communications networks [e.g. Choo (US-6981140-B1)] and information management system [e.g. Yoshioka et al. (US-5909688-A)] and memory management circuit which provides simulated privilege levels [e.g. Johnson et al. (US-5684948-A)] and [e.g. Chris M. Wright ("Proceedings of the Ottawa Linux Symposium")] and method and apparatus providing deception and/or altered operation in an information system operating system [e.g. Cohen et al. (US 20050076237 A1/US 7437766 B2)] and network adapter management [e.g. Choo (US 20030145235 A1)] and [e.g. Paul C. Clark ("Policy-Enhanced Linux")] and [e.g. McIlroy et al. ("Multilevel Security in the UNIX Tradition")].

6. **The following is an examiner's statement of reasons for allowance:**

- The prior art of record does not teach or render obvious the limitations as recited in independent Claims 1, 22, & 41, specific to "a data management unit arranged to associate data management information with data input to the process and to regulate operating system operations involving the data according to the data management information" and "applying a data handling policy upon detecting: (1) a predetermined data type based on a tag or label associated with the data manipulated by the process or based on the format of the data manipulated by the process and (2) one of the predetermined system calls being detected, whereby the data handling policy is applied for all system calls involving the writing of data outside the process" and "the supervisor code controls the process at run time to administer the operating system data management unit" and "associating data management information with data input to the process" and "regulating operating system operations involving the data according to the data management information".
- Dependent claims are allowed as they depend from an allowable independent claim.
- Therefore, the Examiner considers both the above limitations in combination with the remaining limitations as found in each respective independent claim, as applied to the application of data handling policies in an operating system that executes a process, as the non-obvious novelties of the invention.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance".

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Friday from 8:30 AM to 5:00 PM. The examiner can also be contacted via E-mail to schedule a telephone discussion at OSCAR.LOUIE@USPTO.GOV.

If attempts to reach the examiner by telephone or E-mail are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2400 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is only available through Private PAIR. If you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) or 571-272-4100 (local). For more information on the PAIR system or the EBC please visit http://www.uspto.gov/patents/ebc/index.jsp. If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000 (local).

/OSCAR A LOUIE/
11/05/2010

/Nasser Moazzami/
Supervisory Patent Examiner, Art Unit 2436